1

Internet of Things (IoT): Concepts, Issues, Challenges and Perspectives

This chapter is an in-depth review of our article published in 2017. We considered some elements to develop concepts based on the IoT. In this chapter, we present: (1) the connected object (CO), (2) a definition of the Internet of Things, (3) steps and technologies in the IoT ecosystem, (4) IoT to the Internet of Everything (IoE), (5) IoT and Big Data, (6) cloud computing applied to Big Data and the IoT, (7) data science and the IoT, (8) issues and challenges of the IoT, (9) opportunities and threats in the IoT ecosystem, (10) security of the IoT, (11) blockchain and the IoT and (12) conclusion, summarizing the perspectives of the IoT.

1.1. Introduction

The Internet in general and the Web in particular have continued to evolve – from the Web of information to the Web of individualized[1] Things – via various connected objects thanks to miniaturization and technological development, which make room for a double approach: being connected and communicating consistently without any constraints as regards space and time so as to meet the demands and needs of users in terms of services, communication and information [ROX 17, THE 13].

Chapter written by Imad SALEH.

1 In 2011, Vlad Trifa coined the concept of the "Web of Things" (WoT) in his thesis as being the integration of connected objects on the Internet as well as on the Web. This concept is based on the coupling of "social, programmable, semantic, physical and real-time webs, many particular facets that the WoT would have" [ROX 17, p. 38]. Vlad Mihai Trifa, "Building blocks for a participatory Web of Things", thesis, Eidgenössische Technische Hochschule (ETH) Zürich, no. 19890, available at: http://e-collection.library.ethz.ch/view/eth:4641.

The Internet is gradually transforming into a HyperNetwork, just like a network consisting of multitudes of connections between artifacts (physical, documentary), actors (biological, algorithmic), scripts and concepts (linked data, metadata, ontologies, folksonomy), called the "Internet of Things (IoT)", connecting billions of people and objects. It has become the most powerful tool ever invented by man to create, modify and share information. This transformation shows the evolution of the Internet: from a computer network to a network of personal computers, then to a nomadic network integrating communication technologies [CHA 12]. Developments in machine-to-machine (M2M) technologies for remote machine control and the first use of IP (Internet Protocol) in the year 2000 on mobile cellular networks have accelerated the evolution from M2M to the IoT [WOO 11].

1.2. The connected object (CO)

Before defining IoT concepts, it is important to define a connected object as being a device whose primary purpose is neither to be a computer system nor to be a Web Access interface. For example, an object such as a coffee machine or a lock was designed without integrating a computer system or Internet connection. Integrating an Internet connection to a CO enriches it in terms of functionality and interaction with its environment. This makes it an *Enriched CO (ECO)*; for example, the integration of an Internet connection to a coffee machine will make it remotely accessible.

A CO can independently interact with the physical world without human intervention. It has several constraints such as memory, bandwidth or energy usage. It must be adapted for a purpose and has some form of intelligence, which is the ability to receive and transmit data with software through embedded sensors [ROX 17]. A CO has value when connected to other objects and software components; for example, a connected watch is only relevant within a health or wellbeing-oriented ecosystem, which goes far beyond knowing the time.

A connected object (CO) has three key elements:

– generated or received, stored or transmitted data;

– algorithms to process this data;

– the ecosystem in which it will react and integrate.

Use properties of a CO [SAL 17] are:

– ergonomics (usability, workability, etc.);

– aestheticism (shapes, colors, sounds, sensations, etc.);

– usage (cultural history, profile, social matrix, etc.);

– metamorphism (adaptability, customization, modulation, etc.).

Some researchers talk of "hyper objects" [MAV 03] as able to pool their resources to perform everyday tasks as they are linked by "invisible links" within the same ecosystem. In this context, researchers such as [WEI 93] have already considered ubiquitous computing to be where "*the most profound technologies are the ones that have become invisible. Those ones which, when tied together, form the fabric of our daily life to the point of becoming inseparable*" [WEI 91, p. 94].

Communication between objects is passed through identifications that are known to each other. An object must have one or more IDs (barcodes) to be recognized by another so as to establish connection. The GS1 system has proposed a technology based on RFID tags[2] that will uniquely associate the logistical information related to an object with a URL. Google has proposed the Physical Web project to uniquely associate a URL with an object[3]. The ubiquity of heterogeneous, mobile and fragile objects in our life poses the problem of trust models adapted to this complex and fragile ecosystem [SZO 17]. Behind these technologies is the fight for norms and standards for the IoT between giant Internet companies because each wishes to impose its technologies.

1.3. Internet of Things: definition

Kevin Ahston[4], the co-founder of MIT's Auto-ID Center, used the term "Internet Of Things" in 1999. The term IoT was first used during a presentation made by Procter & Gamble (P&G). This term conjures up the

2 RFID is a barcode-like radio-identification process.
3 https://google.github.io/physical-web/.
4 He participated in the creation of the RFID standard.

world of objects, devices and sensors that are interconnected[5] through the Internet.

The CERP-IoT (Cluster of European Research Projects on the Internet of Things) defines the Internet of Things as: "*a dynamic infrastructure of a global network. This global network has auto-configuration capabilities based on standards and interoperable communication protocols. In this network, physical and virtual objects have identities, physical attributes, virtual personalities, intelligent interfaces, and are integrated into the network in a transparent way*" [SUN 10].

This definition presents the two sides of the IoT: the temporal and spatial sides, which allow people to connect from anywhere at any time through connected objects [CHA 12] (Figure 1.1) (smartphones, tablets, sensors, CCTV cameras, etc.). The Internet of Things must be designed for easy use and secure manipulation to avoid potential threats and risks, while masking the underlying technological complexity.

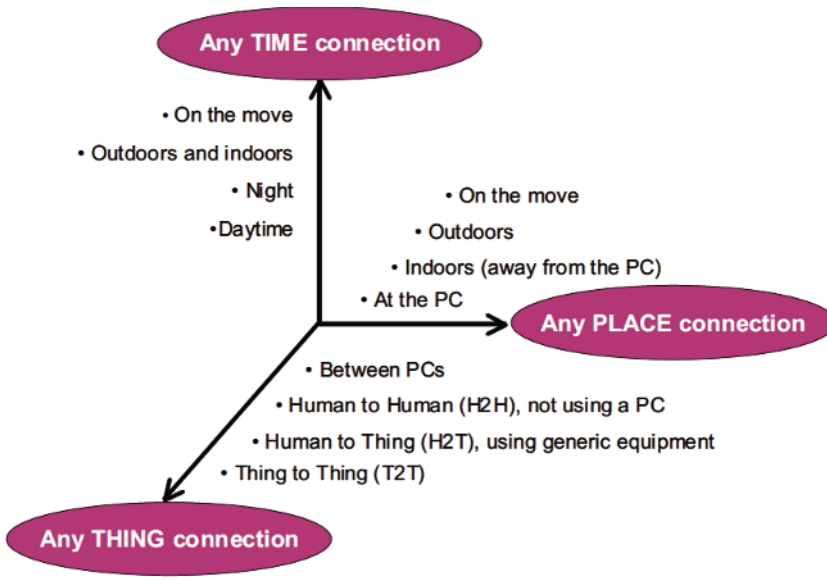

Figure 1.1. *A new dimension for the IoT (source: ITU 2005 [INT 05, taken from [CHA 12])*

5 "That 'Internet of Things' Thing", *RFID Journal*, available at: http://www.rfidjournal.com/articles/view?4986 visited January 2, 2017.

The rapid evolution of this "Internet of Things" shifts the balance between computer and everyday products due to two factors: the generalization of computing resources and the ownership of Web services by users [THE 13].

1.3.1. *Applications*

IoT applications are now practically affecting our day-to-day life such as:

– health and telemonitoring systems to help people;

– connected agriculture to optimize the use of water;

– connected vehicles to help optimize urban traffic management;

– connected appliances to help optimize the consumption and distribution of electrical energy;

– digital arts;

– connected watches for wellbeing and sport.

These examples of applications show that the IoT is integrated into our daily lives and improves people's quality of life [BOU 17a, BOU 17b, NOY 17, AMR 17, GAG 17, CRO 17]. It gives rise to a new market by creating new jobs and trades. It also helps businesses grow, and gives impetus to competitiveness. According to the GSMA [GSM 18], the IoT is a huge growing industry at all hardware and software levels that is expected to provide mobile operators with a comfortable income of about $1200 billion by 2020.

1.4. Steps and technologies in the IoT ecosystem

COs are at the heart of the IoT, but it is necessary to connect all of these objects and enable them to exchange information and interact within the same network. The setting up of the IoT goes through the following steps: identification, sensors setup, object interconnection, integration and network connection. Table 1.1 presents possible steps and protocols [ROX 17].

Identify	Capture	Connect	Integrate	Network
Enabling the identification of each connected element.	Implementing devices that bring the real and virtual worlds closer. The objects basic functions (the temperature sensor for a thermometer, for example).	Establishing a connection between the objects so they can communicate and exchange data.	Using a communication means of connecting objects to the virtual world.	Linking objects and their data to the computing world via a network (the Internet, for example).
IPv4, IPv6	MEMS, RF MEMS, NEMS	SigFox, LoRa	RFID, NFC, Bluetooth, Bluetooth LE, ZigBee, WiFi, cellular networks	CoAP, MQTT, AllJoyn, REST HTTP

Table 1.1. *Steps and technologies to set up the IoT [ROX 17, p. 73]*

1.4.1. *IoT architecture*

Given the rapid development of the IoT, it became necessary to have a reference architecture that would standardize systems design and promote interoperability[6] and communication between the different IoT ecosystems (Figure 1.2 presents the IoT/M2M value chain). For example, an object with the X mark will have to send information to a Y platform via the Z network. Interoperability can be seen from two standpoints, either "closed" within large ecosystems that share the same standards, or "native", based on more global standards, for example, the v1 of the Internet with IP or HTTP.

6 See Frédéric Charles' articles in the journal Zdnet (in French): http://www.zdnet.fr/blogs/green-si/iot-sortir-de-l-internet-des-silos-39855298.htm.

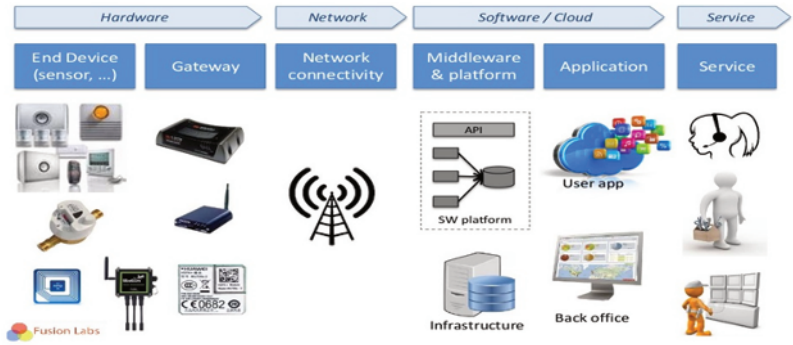

Figure 1.2. *Stéphane Monteil's presentation (January 2016)*[7]

In March 2015, the Internet Architecture Board (IAB)[8] issued the RFC[9] 7452. It proposed four common interaction patterns between IoT actors[10] [see ROX 17, p. 64]:

– *Communication between objects:* this model is based on wireless communication between two objects. Information is transmitted through the integration of wireless communication technology such as ZigBee or Bluetooth.

– *Communication from objects to the cloud:* in this model, data collected by sensors are transmitted to service platforms via a network.

– *Communication from objects to a gateway:* this model is based on an intermediary that links the sensors and applications in the cloud.

– *From objects to back-end data sharing*[11]*:* the purpose of this model is to share data between service providers. It is based on the "programmable web" concept. Manufacturers are implementing an API that allows aggregated data to be used by other manufacturers [ROX 17].

7 "Microsoft Azure IoT Services, architectures, demos", available at: https://www.fusionlabs.fr/language/fr/livres-blancs/.

8 IAB's goal is to ensure Internet development. The organization is divided into working groups, "task forces", including the Internet Engineering Task Force (IETF).

9 Requests For Comments (RFC) are a numbered series of official documents describing the technical aspects of the Internet or different computer hardware.

10 "RFC 7452 – Architectural Considerations in Smart Object Networking", available at: https://tools.ietf.org/html/rfc7452, visited June 11, 2017.

11 The term "back-end" refers to the non-visible part of a software. These are algorithms and other computer processes.

Other organizations offer other types of IoT architectures that prioritize application contexts. The IEEE Standards Association (IEEE-SA) created the IEEE P2413[12] working group that takes into account the variety of IoT application domain contexts. IEEE P2413 has set the following objectives:

– propose a reference model that takes into account relationships, interactions and common architectural elements for various domains;

– develop a reference architecture that is accountable and take into account all areas of applications [ROX 17].

IEEE P2413 proposes a three-level model[13]:

– *Applications*: this concerns applications and services offered to customers.

– *Cloud computing*: this concerns the service platforms for which data is intended. This level makes it possible to establish a link between sensors and platform networks as well as data processing software [ROX 17].

– *Sensor networks*: the lowest level corresponds to sensors and the communication between them (machine-to-machine). This is a network of sensors which generates data and subsequently supplies service offerings [ROX 17].

This model is called "cloud-centric"[14] because it is largely based on the cloud. The IEEE considers cloud computing as a central element for the development of the IoT.

Other companies like the American company Cisco, have proposed layered architectures. In October 2013, Jim Green presented "Building the Internet of Things", the model envisaged by his company for the IoT. It is composed of seven layers (Figure 1.3).

12 "P2413 – Standard for an Architectural Framework for the Internet of Things (IoT)", IEEE SA, available at: https://standards.ieee.org/develop/project/2413.html, accessed June 11, 2017.

13 See Ioan Roxin and Aymeric Bouchereau, "Introduction to the Technologies of the ecosystem of the Internet of Things", in Nasreddine Bouhaï and Imad Saleh (ed.), *Internet of Things: Evolutions and Innovations*, ISTE Ltd, London and John Wiley & Sons, New York, 2017.

14 "Cloud-centric" refers to a concept centered on cloud computing.

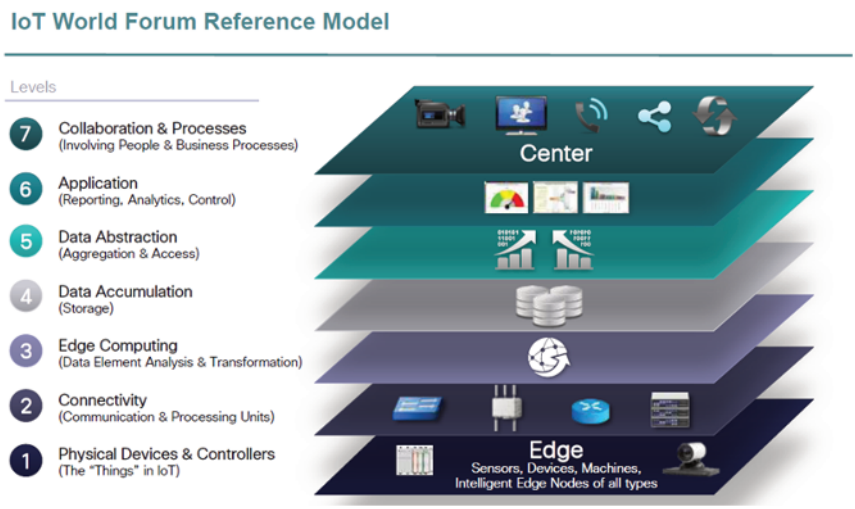

Figure 1.3. *The different layers of the Internet of Things (according to Cisco[15])*

These models show companies' enthusiasm for open and interoperable IoT ecosystem developments to be accepted by market participants. Despite these architectures, much is still to be done to propose a global reference model that takes into account the specificities of the IoT.

1.5. From the IoT to the Internet of Everything (IoE)

According to Cisco[16] [CIS 13], the convergence between the networks of people, processes, data and objects, and the IoT is moving toward the Internet of Everything (IoE) (see Figure 1.4). It is a multidimensional Internet that combines the fields of the IoT and Big Data [INS 15].

15 "Building the Internet of Things | An IoT Reference Model", http://fr.slideshare.net/Cisco/building-the-internet-of-things-an-iot-reference-model.
16 http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/everything-for-cities.pdf.

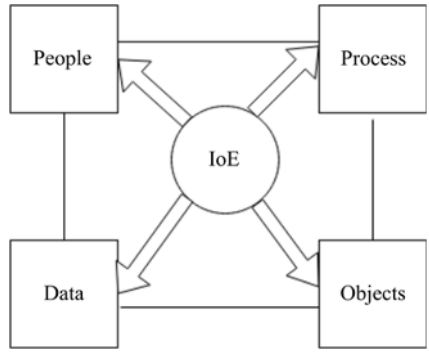

Figure 1.4. *Internet of Everything (IoE)*

"*People:* Connect people in a more relevant way and with more value.

Process: Provide the right information to the right person (or machine) at the right time.

Data: Rely on data to bring out the most useful information for decision-making.

Objects: Physical devices and objects connected to the Internet for intelligent decision-making". (Source: [CIS 13], taken from [INS 15]).

The IoE presents a broader vision of the IoT as the network is distributed and decentralized. It is equipped with artificial intelligence at all levels to better protect networks and allow the user to have personalized data, which helps in decision-making. This is a marketing idea of the IoE.

1.6. IoT and Big Data

Big Data[17] is a huge volume of digital data generated by Internet users, connected objects and so on. Big Data is at the heart of IoT development. Without this data, COs remain as physical devices unconnected to the real

17 According to the archives of the digital library of the Association for Computing Machinery (ACM), the term "Big Data" appeared in October 1997, in scientific articles dealing with technological challenges with the aim of visualizing "large data sets" [ROX 17, p. 48].

world. Big Data is a global concept which refers to six variables (6Vs) [ROX 17, p. 48]:

– *volume*: this relates to the volume of generated data;

– *variety*: this relates to data types, namely raw, semi-structured or unstructured data, coming from several sources such as the Web, connected objects and networks;

– *speed or velocity*: this relates to the frequency of generated, captured and shared data;

– *veracity*: this relates to the reliability and credibility of collected data;

– *value*: this relates to the advantages derived from the use of Big Data;

– *visualization*: this relates to the restitution of information, so that it is comprehensible and interpretable in spite of its volume, structure, source and constant evolution [ROX 17].

Today, we know where, when and who produces structured data or not (Big Data). These clarifications make "*the success of Twitter which, in addition to the textual content of the message, encapsulates spatio-temporal information and by crossing with the profile of the author, adds information on a particular social network*" [SZO 12]. This poses significant epistemological and methodological problems [BOY 12, RIE 12] with regard to the multiplication of "micro-interpretations" of data and their representation [SZO 12].

These data play an important role in the economic development of companies. The analyses of "digital traces" left by the use of the Internet allow us to personalize the service suitably for the user's profile and location. Data produced by connected objects can provide information about user habits, skills or relationships. Digital companies have already understood the importance of controlling user traces and increasing their number. Some companies offer to control this data and identify objects. This raises ethical and authenticity issues for the user of produced data. In this context, the more objects possess intelligent algorithms to perceive and act, the more they become autonomous and increase problems related to private life. It is therefore important to develop technologies to allow objects to have *auto-immunity* against malicious codes or unauthorized penetrations to prevent data propagation or erroneous codes. Data can be located and stored

in a centralized or globalized database, in databases distributed using cloud computing technologies.

Some data may or may not be useful, but the major challenge lies in contextualizing this data to make sense of it, so as to create value for users and businesses. Data transmitted by the IoT are raw and unprocessed materials, which are useful when they are combined and processed to form meaningful information. It is necessary to filter data for their utility knowing that data may be useful for some processes but not for others. The role of intelligent algorithms can be a solution to filter the relevance of data. Nevertheless, it is difficult to systematically transform this huge data into information and subsequently into knowledge that can be used in everyday life. One approach consists of semantically enriching these data through ontologies to facilitate their reuse and to allow the implementation of reasoning mechanisms [SEY 15]. Moreover, if knowledge is complemented by experiments, data will be transformed into knowledge and will enrich the abilities of the IoT ecosystem (Figure 1.5). Data generated or produced by the IoT raises questions regarding their owners and the right to them.

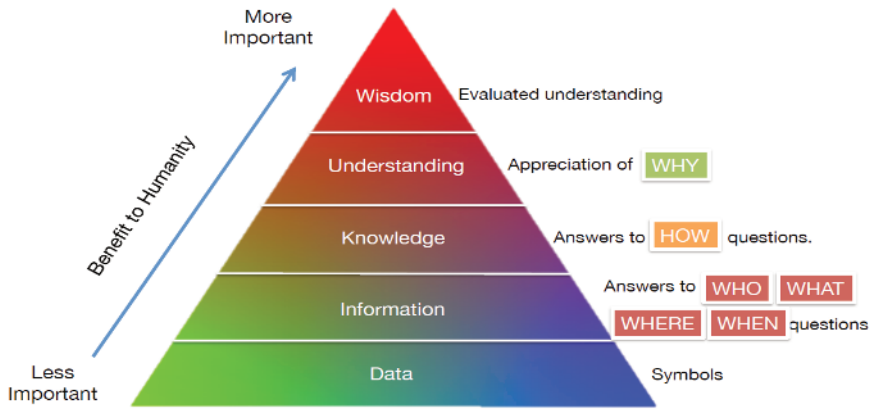

Figure 1.5. *Slide 11, taken from the presentation of Bob Gill, P.Eng., FEC, smIEEE, November 29, 2016. For a color version of this figure, see www.iste.co.uk/saleh/challenges.zip*

1.7. Cloud computing applied to Big Data and the IoT

Cloud computing platforms will store, retrieve and analyze data from remote servers. "*Cloud computing applied to Big Data and the IoT allows the centralization of data and processing power. Cognitive analysis and automatic learning techniques* [*machine learning*] *are among the 'tools' that exploit large volumes of data*" [ROX 17, p. 49]. Research in the cognitive field and the improvement of learning techniques necessarily contribute to the development of the IoT and the best exploitation of data generated by objects. [ROX 17, p. 49]

1.8. Data science and the IoT

Data science is a science capable of providing a necessary foundation for Big Data [PIN 17, p. 132]. It makes data permanently generated by the visual and interpretable IoT.

It is based on techniques such as *data mining, machine learning, visual analytics, cloud computing, parallel computing and information retrieval* [PIN 17, CIT 18]. Data science deals with data processing and the visualization process in all areas based on the constant flow of data such as transportation, insurance and health [PIN 17].

Data science precisely defines the current forms of analytical visualization [PIN 17]. Data visualization is a fundamental step in identifying models, trends and relationships between data using Big Data. Visualization allows the emergence of the field of study called *visual analytics*, which is based on "*the use and interactive visual analysis of large and complex data (dataset)*" [PIN 17]. It "*represents the analytical process and requires a high degree of monitoring and human–machine interaction*" [PIN 17, p. 132]. Data science makes it possible to discover new algorithms for data visualization [CHE 15].

Figure 1.6 summarizes the relationship between the technologies described below and the IoT [NOY 17].

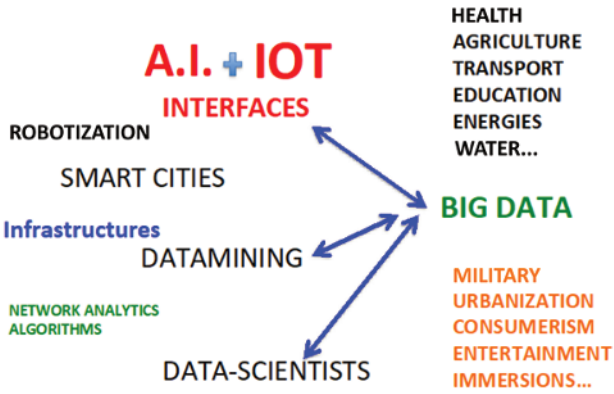

Figure 1.6. *Taken from Jean-Max Noyer's article [NOY 17]*

1.9. Stakes and challenges of the IoT

The IoT affects all areas of the co-construction of knowledge, from the management of companies and administrations through to educational and hyper-urban technologies. It transforms our localized relationship into a globalized relationship by transcending geographical boundaries [SAL 12, SAL 14]. These technological, societal and human transformations raise many questions about societal and economic change, as well as research, creativity and innovation. It is important to think of building new instruments for a technical future at the service of human development.

1.9.1. *Technological challenges*

The IoT is at the center of all modern technological developments, where the issue of interfaces and protocols in a major strategic situation is raised. "*All information, be it textual, sound or visual [and also input gesture] is in constant interaction with all the others, it becomes reticular*"[18]. The IoT transforms the Internet into a globalized HyperNetwork with all its points of forming as many information nodes as possible without borders [SAL 12, SAL 14].

18 Jean-Pierre Balpe, available at: http://hyperfiction.blogs.liberation.fr/2007/10/25/des-hypertextes/, visited January 10, 2018.

Challenges in terms of computer programming are immense. New methods of design, development, debugging and maintenance must be set up. From innovative symbolic languages, future computer scientists will transform simple code lines into autonomous agents that are capable of existing in the complexity of ubiquitous and distributed systems, to adapt to users' demands in order to recommend new uses or even accompany them in the evolution of their modes of existence.

A major challenge for the IoT at the technical and functional level is to manage technological heterogeneity and standards of objects coupled with multitudes of application needs and uses in terms of security services. It should be noted that these needs can evolve over time depending on the context and taste. In fact, how do we ensure individual authentication of several million heterogeneous objects, equipped with heterogeneous communication technologies, across multiple administrative domains? [VER 11]. This raises managerial issues and the security of objects in a heterogeneous environment at the physical and logical level. "*In fact, the Internet of Things is a complex system in which people interact with a technological ecosystem based on smart objects and through complex processes. The interaction of these four components of the IoT (people, smart objects, technological ecosystem, processes) are giving rise to a systemic dimension to the security of the IoT*" [CHA 12, p. 54]. Therefore, tensions on the security of the IoT are created during the interaction of smart objects with its environment. These tensions (*trust, responsibility, identification and autoimmunity*) are characterized by a cognitive and systemic dimension induced by the growing autonomy of objects [CHA 12].

1.9.2. *Societal challenges*

The challenge for the future will be to respond as creatively as possible to anthropological concerns, climate regime shifts, biodiversity, industrial implications and energy transition, bio-political involvement as well as ethics of accessibility, cultural diversity and redefinitions of the notion of "personal data". However, questions are also raised concerning the dissemination of intellectual technologies as counterpowers in a centric data society, by proposing models of analysis, conceptual frameworks equal to what is advanced, design methods and rules of usage recognized by all users and by new collective intelligence of usage.

1.9.3. *Environmental challenges*

The constantly increasing number of connected objects has consequences on the environment. It can be translated from the increase in electronic waste and their recycling, on the one hand, and energy consumption, on the other hand. This is a major challenge that is attracting more and more governments to study the impact of connected objects on global warming and their impact on populations. For example, the European Union[19] has set a 2020 target to reduce CO_2 emissions by 20% and improve energy efficiency by 20% in order to attain 20% renewable energy. It is therefore necessary that, before manufacturing COs, companies study their service lifespan and usefulness for users in order to reduce the production of unnecessary objects and unnecessary energy consumption.

1.9.4. *Confidence in the IoT*

Thus, the degree of confidence in the IoT and its acceptance are prerequisites for the implementation of adequate measures for personal data protection and private life. As a matter of fact, it is important to provide all user requirements and data security when designing IoT elements [EUR 09]. There are solutions based on cryptography or pre-distribution key management that could accommodate object resource constraints [CHA 12]. Nevertheless, questions are raised about the robustness of such solutions to an IoT that potentially comprises millions of objects.

1.9.5. *Challenges for businesses*

The IoT is constantly growing: “the invisible memory” of the web is based on the traces left by users registered in databases and analyzed by means of statistical and other methods. We feel that it is important that public or private actors seize the opportunity of the evolution of the IoT and this memory to propose unique approaches for the wellbeing of humanity.

– For businesses, it is important to understand user behavior and consumer trends in order to provide tailored services and products.

19 Website: https://ec.europa.eu/clima/policies/strategies/2020_fr, visited February 4, 2018.

– Political actors can follow company trends in order to adjust their methods of organization and values, while adapting their programs and their mode of operation.

1.9.6. *Challenges for researchers*

– Researchers in humanities and social sciences (HSS) have "total" fantastic observation means that aim "to revolutionize classical methodologies by eliminating the division between micro and macro, between qualitative and quantitative" [RIE 10].

– Researchers in other sciences (computer science, mathematics, etc.) have a quantity of data to test the reliability, speed and invention of algorithms.

– Researchers in MMI have data and tools that allow them to imagine and create aesthetic and understandable artifacts to visualize data, which is received almost continuously [PIN 17].

"*The quantity and wealth of data would suggest that we can move, through a kind of 'zoom', from the whole to the individual and from average to idiosyncrasy*" [RIE 10]. The processing and analysis of digital traces and data produced by the IoT are changing both the ways in which researchers produce and communicate knowledge, and the organization of research, its economy as well as its role in society [RIE 10].

The IoT raises a number of epistemological and sociotechnical problems: freedom–control, authority–independence, associativity–uniqueness, automatism–control, actions–interactions, contextualization–decontextualization, adaptivity–integrity, etc. We must now learn to "*think of the mobile, the vague, the uncertain, the near and the distant*"[20].

1.10. Opportunities and threats in the IoT ecosystem

We can notice that applications and services developed around the IoT are likely to improve daily life, by optimizing and automating certain activities. On the other hand, some IoT-related questions arise on the usage

20 Jean-Pierre Balpe, "Des hypertextes à l'hypermonde", available at: http://nt2.uqam.ca/fr/actualites/des-hypertextes-l'hypermonde, accessed December 6, 2016.

and control of information to prevent hacking, user-abusive surveillance, etc. In Table 1.2, we summarize the opportunities and threats which IoT developments pose at the technical, human and socio-economic levels.

Opportunities	Threats
Fast-growing market	Difficult market access for small companies
Reduction of the cost of technologies	Physical frailty of objects
Competitiveness that fosters innovation	Influence on decision-making to guide innovation
Technological development (Ipv6, miniaturization)	Lack of norms and standards
Increased connection speed	Technological fracture
Improvement of daily life	Political and social manipulation
Connection everywhere without constraints of space and time	Abusive surveillance Environmental impact
Permanent flow of data	Security, protection and data control

Table 1.2. *Opportunities and threats*

1.11. IoT security

Given the emergence of IoT technologies in all areas of everyday life, questions about IoT security are bound to arise. It must be considered from three complementary angles: *technological, human and systemic* [CHA 12]:

– *Technology protection* concerns data security, communications and infrastructure networks as well as their functionality.

– The protection of individuals concerns the protection of the private lives of users (“privacy”) to avoid disputes that are likely to be caused by the IoT.

– "*The protection of interconnected systems hosting IoT objects will concern the protection of objects themselves delivered to these systems and the processes they control*" [CHA 12, p. 62].

Yacine Challal [CHA 12] analyzed existing research and the needs of the IoT in terms of security and he concluded that potential developments can be seen around three areas: in the short, medium and long term. In Table 1.3, he illustrates these three areas and summarizes the scientific and technological barriers behind each of them.

Systemic and cognitive approach to IoT security	– Trust models for "object storage" – Autoimmunity of objects – Identification – Responsibility
IT security **Omnipresent mobile**	– Privacy and user-centric security according to the context – Adaptive management of profiles and security policies – Security sharing in the mobile network
Safety of miniaturized embedded networks	– Effective cryptography for embedded computing – Effective and scalable key management – Authentication and effective management of credentials – Secure protection for LLN environments
IoT security	– Technology protection – Protection of individuals – Systems protection

Table 1.3. *Three major projects for security and privacy in the IoT ([CHA 12, p. 63]; we have only modified the presentation)*

1.12. Blockchain and the IoT

1.12.1. *Definition*

Blockchain is a technology developed for the Bitcoin cryptocurrency by Satoshi Nakamoto (pseudonym) in 2008 [NAK 08]. Blockchain France has defined blockchain as "*an information storage and transmission technology, which is transparent, secure, and operates without a central control body. By extension, a blockchain is a database that contains the history of all transactions made between its users since its creation. This database is secure and distributed: it is directly shared by its different users, allowing everyone to check the validity of the chain*[21]".

Blockchain[22] is a distributed registry system where transaction logging is done across multiple nodes in a peer-to-peer (P2P) network.

"Commotion" (http://commotionwireless.net/) and "Blockchain" variations are of decentralized systems. The aim is to break away from the central body by putting in place devices that work independently of a central entity. Moreover, there are political problems that go with it as part of a society of hyper-control[23].

1.12.2. *Operation*

"*Any public blockchain must operate with a programmable currency or token*[24]", Bitcoin being an example. Bitcoin users, who know each other by exchanging public keys, generate and distribute transactions on the network to transfer money. These transactions are grouped together in a block by users. When a block is filled, it is added to the blockchain after a mining process. To mine a block, network nodes, called "minors", try to solve a cryptographic problem called "Proof-of-Work (PoW)". "*Once the block is validated, it is time-stamped and added to the Blockchain*[25]". At this point,

21 Taken from the Blockchain website: https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/, visited January 30, 2018.
22 See Ahmed Banafa's blog, available at: https://ahmedbanafa.blogspot.com/ (accessed January 30, 2018), for more information.
23 Serge Abiteboul, "S'affranchir de l'autorité centrale avec la blockchain", *La Recherche*, November 2017.
24 Also from the Blockchain website, visited January 30, 2018.
25 Also from the Blockchain website, visited January 30, 2018.

the transaction is visible to the receiver as well as to the entire network (Figure 1.7).

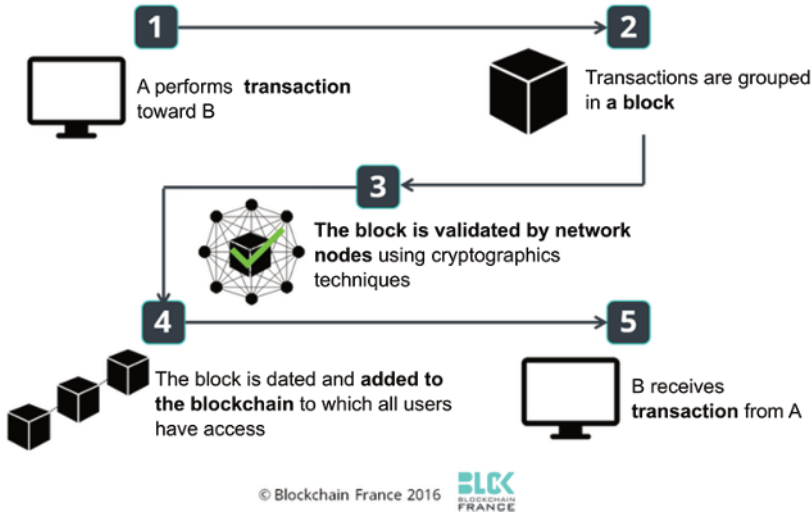

Figure 1.7. *Taken from the company website: https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/ (we respected the original figure but the explanations have been translated from French to English)*

In the context of the Internet of Things and because of the interconnection of heterogeneous systems that generate a large volume of personal data, our digital company faces a number of challenges (see below). Given the functioning of distributed blockchain and its consensus mechanisms that reconcile divergent interests and distributed trust through the removal of the single trusted third party, it can offer answers to certain challenges.

However, as stated by Dorri *et al*. [DOR 16], adapting this technology to the IoT is not an easy task. In fact, the mining process requires high computing capacity while the majority of IoT devices have limited resources. Moreover, this process takes time, whereas in most IoT applications, low latency is desirable. In addition, blockchains become difficult to use as the number of nodes in the network increases, while IoT networks should contain a large number of nodes. Finally, the underlying protocols of blockchains create significant indirect traffic which may pose problems for some IoT devices with limited bandwidth [DOR 16].

1.12.3. *Applications*

In this context, many researchers have studied the use and adaptation of blockchain in the IoT. Among them is Mettler [MET 16] who illustrates the use of this technology in the field of health, be it for public health management, medical research based on patients' personal data or for quality assurance in the production of drugs. Moreover, Dorri *et al*. [DOR 17] presented an adaptation of blockchain for the case of smart homes. By grouping devices into clusters and adding local blockchains, they show that it is possible to reduce the load on the network while ensuring the security of user data and the protection of their private lives. Finally, in an article [CHR 16], Christidis *et al*. expose the use of blockchain technology for smart contracts. These smart contracts are "*stand-alone programs that automatically execute the terms and conditions of a contract, without requiring human intervention once started*[26]". Smart contracts can be interesting for the IoT because they allow the automation of long processes, while ensuring their verifiability.

The integration of blockchain into the IoT will lead to significant transformations in several sectors, leading to new models that will require us to reconsider how existing systems and processes are implemented. Blockchain can also be a means of ensuring the security of user data as well as the protection of private life, thus allowing for greater adoption of the IoT[27].

1.13. Conclusion

In a world that is "hyper-connected" through connected objects where users are both transmitters and receivers of data, the IoT opens new fields to explore for the information and communication sciences to, on the one hand, study societal challenges of these new technological and digital transformations, and on the other hand, analyze whether connected objects meet the needs of users who are increasingly demanding in terms of service, communication and information. The IoT must be approached from two

26 Also taken from the Blackchain website, visited January 30, 2018.

27 This section was written in January 2018, in collaboration with Amri Toumia, a PhD student.

angles: on the one hand, the industrial and technological reality of connected objects, such as business management, e-administration, e-government and gestures (pedometer, gaze direction, GPS, etc.); and on the other hand, the impacts of connected objects in everyday life, for example on health, housing, cars, insurance, etc.

Figure 1.8 illustrates, according to us, the future developments of the IoT.

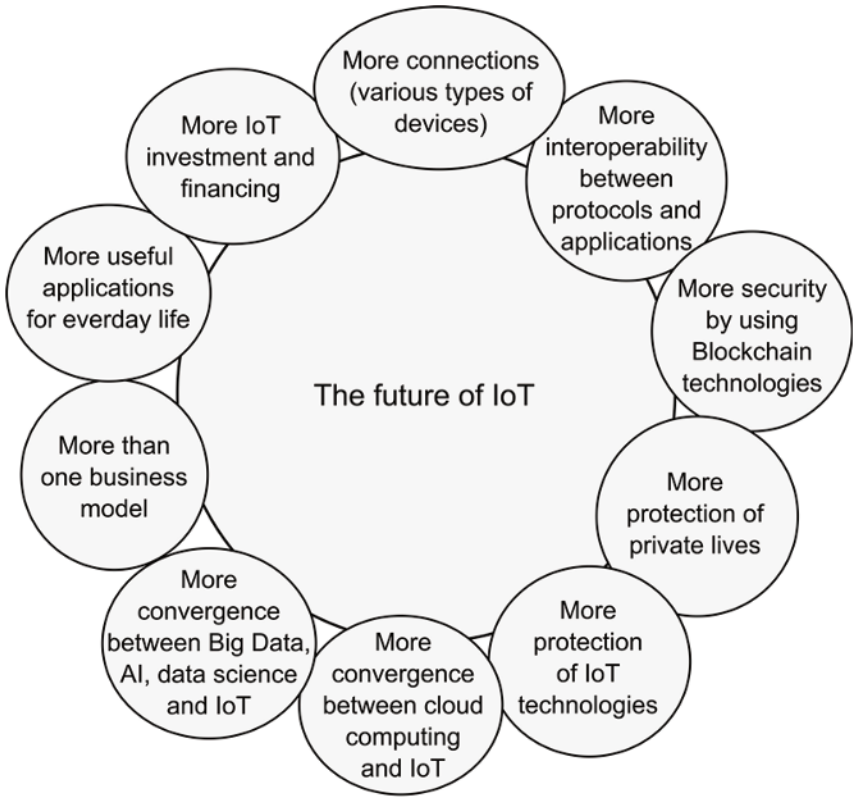

Figure 1.8. *The future of the IoT*

1.14. References

[AMR 17] AMROUM H., TEMKIT M'H., AMMI H. *et al.*, "Apprentissage en profondeur des données brutes de l'activité humaine", *Internet of Things*, vol. 2, no. 2, ISTE OpenScience, 2017.

[BOU 17a] BOUHAÏ N., SALEH I. (eds), *Internet of Things: Evolutions and Innovations*, ISTE Ltd, London and John Wiley & Sons, New York, 2017.

[BOU 17b] BOUHAÏ N., "The IoT: intrusive or indispensable objects?", in BOUHAÏ N., SALEH I. (eds), *Internet of Things: Evolutions and Innovations*, ISTE Ltd, London and John Wiley & Sons, New York, 2017.

[BOY 12] BOYD D., CTAWFORD K., "Critical question for big data", *Information, Communication & Society*, available at: https://people.cs.kuleuven.be/~bettina.berendt/teaching/ViennaDH15/boyd_crawford_2012.pdf (accessed February 2, 2017), 2012.

[CHA 12] CHALLAL Y., "Sécurité de l'Internet des Objets : vers une approche cognitive et systémique", Thesis, UTC, June 2012.

[CHE 15] CHEN L.M., SU Z., JIANG B., *Mathematical Problems in Data Science: Theoretical and Practical Methods*, Springer International Publishing, Amsterdam, 2015.

[CHR 16] CHRISTIDIS K., DEVETSIKIOTIS M., "Blockchains and smart contracts for the Internet of Things", *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[CIT 18] CITY UNIVERSITY OF LONDON, MsC in Data Science Course, available at: https://www.city.ac.uk/courses/postgraduate/data-science-msc (accessed on February 6, 2017), 2018.

[CRO 17] CROUZY S., BORKOWSKI S., COQUILLART S., "Ambient Atoms : un périphérique pour la visualisation ambiante d'informations", *Internet of Things*, vol. 2, no. 2, ISTE OpenScience, 2017.

[DOR 16] DORRI A., KANHERE S.S., JURDAK R., "Blockchain in Internet of Things: challenges and solutions", *arXiv*, eprint arXiv:1608.05187, August 2016.

[DOR 17] DORRI A., KANHERE S.S., JURDAK R. *et al.*, "Blockchain for IoT security and privacy: the case study of a smart home", *IEEE International Conference on Pervasive Computing and Communications Workshops*, March 2017.

[EUR 09] EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, Internet of Things – an action plan for Europe, 2009.

[GAG 17] GAGNERÉ G., PLESSIET C., SOHIER R., "Espace virtuel interconnecté et Théâtre. Une recherche-création sur l'espace de jeu théâtral à l'ère du réseau", *Internet of Things*, vol. 2, no. 2, ISTE OpenScience, 2017.

[GSM 18] GSMA, available at: https://www.gsma.com/, 2018.

[INT 05] INTERNATIONAL TELECOMMUNICATION UNION, "Ubiquitous Network Societies: their impact on the telecommunication industry", *ITU Workshop on Ubiquitous Network Societies*, April 2005.

[MAV 03] MAVROMMATI I., KAMEAS A., "The evolution of objects into hyper-objects: will it be mostly harmless?", *Personal and Ubiquitous Computing*, vol. 7, nos 3–4, pp. 176–181, available at: http://dx.doi.org/10.1007/s00779-003-0223-1, 2003.

[MET 16] METTLER M., "Blockchain technology in healthcare: the revolution starts here", *IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–3, 2016.

[MIT 13] MITCHELL S., VILLA N., STEWART-WEEKS M. *et al.*, *The Internet of Everything for Cities*, Cisco, 2013.

[INS 15] INSTITUT MONTAIGNE, Big data et objets connectés – faire de la France un champion de la révolution numérique, Report, April 2015.

[NAK 08] NAKAMOTO S., Bitcoin: a peer-to-peer electronic cash system, 2008.

[NOY 17] NOYER J.-M., "L'Internet des Objets, l'Internet of Everything : quelques remarques sur l'intensification du plissement numérique du monde", *Internet of Things*, vol. 1, no. 1, ISTE OpenScience, 2017.

[PIN 17] PINTOA A.L., GONZALES-AGUILAR A., DUTRA M.L. *et al.*, "The visualization of information of the Internet of Things", in BOUHAÏ N., SALEH I. (eds), *Internet of Things: Evolutions and Innovations*, ISTE Ltd, London and John Wiley & Sons, New York, 2017.

[RIE 10] RIEDER B., "Pratiques informationnelles et analyse des traces numériques : de la représentation à l'intervention", *Etudes de communication*, no. 35, pp. 91–104, available at: https://edc.revues.org/2249 (accessed on February 3, 2017), 2010.

[RIE 12] RIEDER B., RÖHLE T., "Digital methods: five challenges", in BERRY D.M. (ed.), *Understanding Digital Humanities*, Palgrave Macmillan, Houndmills, 2012.

[ROX 17] ROXIN I., BOUCHEREAU A., "The ecosystem of the Internet of Things", in BOUHAÏ N., SALEH I. (eds), *Internet of Things: Evolutions and Innovations*, ISTE Ltd, London and John Wiley & Sons, New York, 2017.

[SAL 12] SALEH I., HACHOUR H., "Le numérique comme catalyseur épistémologique", *Revue Française des Sciences de l'Information et de la Communication*, no. 1, available at : http://rfsic.revues.org/168, 2012.

[SAL 14] SALEH I., HACHOUR H., BOUHAÏ N., *Les frontières numériques*, L'Harmattan, 2014.

[SAL 17] SALEH I., "Les enjeux et les défis de l'Internet des Objets (IdO)", *Internet of Things*, vol. 1, no. 1, ISTE OpenScience, 2017.

[SEY 15] SEYDOUX N., BEN ALAYA M., HERNANDEZ N. *et al*., "Sémantique et Internet des objets : d'un état de l'art à une ontologie modulaire", *26es Journées francophones d'Ingénierie des Connaissances*, Rennes, available at: https://hal.archives-ouvertes.fr/IC-2015/hal-01166052 (accessed on March 3, 2017), June 2015.

[SUN 10] SUNDMAEKER H., GUILLEMIN P., FRIESS P. *et al*. (eds), *Vision and Challenges for Realising the Internet of Things*, Cluster of European Research Projects on the Internet of Things, 2010.

[SZO 12] SZONIECKY S., Evaluation et conception d'un langage symbolique pour l'intelligence collective, vers un langage allégorique pour le Web, Thesis, University of Paris 8, December 2012.

[SZO 17] SZONIECKY S., SAFIN S., "Modélisation éthique de l'Internet des Objets", *Internet of Things*, vol. 2, ISTE OpenScience, 2017.

[THE 13] THEBAULT P., La conception à l'ère de l'Internet des Objets : modèles et principes pour le design de produits aux fonctions augmentées par des applications, Thesis, ParisTech, 2013.

[VER 11] VERMESAN O., FRIESS P., GUILLEMIN P. *et al*., "Internet of Things Strategic Research Roadmap", in VERMESAN O., FRIESS P. (eds), *Internet of Things – Global Technological and Societal Trends*, River Publishers, 2011.

[WEI 91] WEISER M., "The computer for the XXIe century", *Scientific American*, vol. 265, no. 3, pp. 3–11, 1991.

[WEI 93] WEISER M., "Hot topics: ubiquitous computing", *IEEE Computer*, October 1993.

[WOO 11] WOOD L., "Today, the Internet, tomorrow – the Internet of Things", *Computer World*, available at: http://www.computerworld.com/s/article/9221614/Today_the_Internet_tomorrow_the_Internet_of Things, November 2011.